

REMARKS/ARGUMENTS

Favorable reconsideration of this application, in light of the present amendments and following discussion, is respectfully requested.

Claims 1-22 are pending in this case. Claims 1, 2, 4, 5, 7, 8, 11, 14, 15, and 20-22 are amended by the present amendment. The changes to Claims 1, 2, 4, 5, 7, 8, 11, 14, 15, and 20-22 correct matters of form and are also supported in the originally filed disclosure at least at Figures 2, 3, and 17 and at paragraphs [0155], [0158], and [0162]. Thus, no new matter is added.

In the outstanding Office Action, Claims 1-4, 14-17, and 22 were rejected under 35 U.S.C. § 103(a) as unpatentable over Asano, et al. (EP 1185020 A1, herein "Asano1") in view of Oishi, et al. (EP 1039462 A2, herein "Oishi"), further in view of Shindo, et al. (U.S. Pub. No. 2003/0065925, herein "Shindo"); Claims 5, 6, 18, and 19 were rejected under Asano1 in view of Asano, et al. (U.S. Pub. No. 2002/0085722, herein "Asano2"), further in view of Shindo; and Claims 7, 8, 20, and 21 were rejected under 35 U.S.C. § 103(a) as unpatentable over Asano2 in view of Asano1; and Claims 9-13 were rejected under 35 U.S.C. § 103(a) as unpatentable over Asano1 in view of Oishi.

At the outset, Applicants note that, at page 2, the outstanding Office Action asserts that "Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection." However, **several assertions made in the previous Office Action are maintained in the outstanding Office Action without responding to Applicants' previous arguments directed to those repeated assertions.** For example, the **arguments in the previous response that Asano1 and Oishi are not properly combined are not responded to** but the combination of Asano1 and Oishi is again asserted by the outstanding Office Action. The **bases for the rejections of Claims 7-13, 20, and 21 are exactly the same as in the previous Office Action with no response to Applicants'**

previous arguments. Applicants note that, not only does the failure of the outstanding Office Action to respond to previous arguments derogate MPEP § 707.07(f) and MPEP § 2142, but it also prevents Applicants from advancing the prosecution of the claimed invention.

Applicants respectfully request that any subsequent action fully consider and respond to the remarks herein.

Applicants respectfully traverse the rejections under 35 U.S.C. § 103(a).

Response to Rejections of Claims 1-6, 14-19, and 22

The outstanding Office Action concedes, at page 5, that Asano1 and Oishi do not teach “acquiring a second seed by decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1,” which is defined by Claim 1 as generated based on a first seed. However, Shindo is asserted for the above-quoted feature of Claim 1.

Shindo describes an information recording apparatus that encrypts information. At paragraph [0009], Shindo describes a system in which audio-visual data is divided into equal-size blocks. Each block is encrypted by a key calculated from a seed, where a signal representing the seed is encrypted by a public-key cryptosystem. Each data block is encrypted by a single key, but the order in which the keys are used may be, for example, alternately an odd key followed by an even key. As described at paragraph [0086], during information reproduction, the CPU 23 controls read out of the encryption-resultant signal of a seed 19. The signal is decrypted to obtain the original signal of the seed 19, which is fed to the decryption controller 62.

However, as is clear from the description above, Shindo does not cure the deficiencies of Asano1 and Oishi with regard to “acquiring means for **acquiring a second seed by**

decrypting an encrypted second seed stored on said information-recording medium **on the basis of said generated first block key Kb1,”** as recited by Claim 1, because **in Shindo**, a **first block key Kb1 is not the basis for acquiring the signal of the seed 19**. Instead, a public-key cryptosystem is used to encrypt the signal representing the seed 19, and that signal is decrypted by the CPU 23, as described at paragraph [0086].

Applicants have previously submitted arguments that Asano2 and Oishi are not properly combined under MPEP § 2143.01, and, therefore, a prima facie case of obviousness has not been established with regard to Claims 1-4. Applicants request that those remarks be considered and a proper response set out.

More importantly, **none of Asano2, Oishi, and Shindo teaches or suggests acquiring a second seed on the basis of any type of first key block**, let alone a generated first key block, which is generated on the basis of a first seed, as defined by Claim 1. Thus, the combination of the references necessarily fails to teach or suggest the above-discussed features of Claim 1, as well.

Because, even in combination, Asano2, Oishi, and Shindo fail to teach or suggest at least the above-discussed features of Claim 1, Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) of Claim 1 and Claims 2-4, which depend therefrom, be withdrawn.

Claims 14 and 22, though differing in scope and statutory class from Claim 1, patentably define over the combination of Asano2, Oishi, and Shindo for similar reasons as Claim 1, at least with regard to the features of Claim 1 discussed above. Thus, Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) of Claim 14, Claims 15-17, which depend therefrom, and Claim 22 be withdrawn.

Claims 5 and 18, though differing from Claim 1 in scope and statutory class, include “each encryption-processing unit...configured to...**acquire a second seed by decrypting an**

encrypted second seed...on the basis of said generated first block key Kb1” and “acquiring a second seed...by decrypting an encrypted second seed...on the basis of said generated first block key Kb1,” respectively. Shindo, which is asserted to teach the above-quoted features of Claims 5 and 8, at page 11 of the outstanding Office Action, is already discussed above as failing to do so. As noted above, Shindo, instead describes a signal of the seed 19 being decrypted by the CPU 23. The seed 19 is neither a second seed nor acquired based on a first block key, generated based on a first seed, as defined by Claims 5 and 18.

Further, Asano1, which is asserted instead of Oishi against Claims 5 and 18, fails to cure the deficiencies of Shindo with regard to the above-quoted features of Claims 5 and 18, and, further, is not asserted for the above-quoted features.

Thus, Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) of Claim 5, Claim 6, which depends therefrom, Claim 18, and Claim 19, which depends therefrom, be withdrawn.

Response to Rejection of Claims 7, 8, 20, and 21

The rejection of Claims 7, 8, 20, and 21 is repeated from the previous Office Action, with no discussion of Applicants’ previously filed arguments. Thus, Applicants respectfully request that the following arguments be fully considered and, if the rejection is maintained, the arguments be specifically addressed in any subsequent action.

With regard to independent Claims 7, 8, 20, and 21, the outstanding Office Action asserts that Asano2 teaches “carrying out an authentication process...to generate a session key Ks.”

As understood by anyone of ordinary skill in the pertinent art, **a session key is a single-use key for a specific session** or use.

Asano2 is completely silent regarding a session key. As stated at the Abstract of Asano2, a content-cryptosystem key is generated with secret information, such as a stamper ID stored beforehand on a recording medium, a master key, and a media key. None of the content-cryptosystem key, master key, media key or any key discussed by Asano2 is a session key that is specific to a session. As described at paragraph [0043] of Asano2, a master key is common to a plurality of information recording devices, and a media key is unique to a specified recording medium. Further, neither the master key nor the media key is generated via an authentication-processing unit. The resulting content-cryptosystem key is a key controlling use of the content, for every session or use involving the content. Thus, Asano2 does not teach or suggest generation of a session key.

In the Response to Arguments, at page 4, the Office Action dated September 19, 2008 asserts that “Asano2 discloses that B received encrypted data from A and authenticates A (i.e. authentication process) and then B generates a session key (0449, lines 1-2, 10-11; 0450, lines 1-3).” However, as Applicants argued in the previous response, neither paragraphs [0449], [0450], nor any other portions of Asano2 make any reference to a session key.

Asano1 does not cure the deficiencies of Asano2 with regard to the above-discussed features and, further, is not asserted to teach generation of a session key.

Thus, Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) of Claims 7, 8, 20, and 21 be withdrawn.

Response to Rejection of Claims 9-13

With regard to claim 9, Asano1 is conceded not to teach, and Oishi is asserted to teach “**generating**, outside the information-recording medium, **a second seed** serving as key generation information encrypted **on the basis of a first block key Kb1 generated on the basis of said first seed**” and “**generating, outside the information-recording medium, an**

encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed; and storing said encrypted content in the information-recording medium.”

Oishi, at paragraph [0014], describes:

In a storage device, encrypted digital data and a storage encrypted content key are transmitted to the data processing apparatus

In the data processing apparatus, the storage encrypted content key is extracted using a session key and transmitted to the storage device

In the storage device, the extracted storage encrypted content key is decrypted back to a content key by a storage use key and re-encrypted to a session encrypted content key by a session key

In the data processing apparatus, the session encrypted content key is decrypted back to content key with the session key

In the data processing apparatus, the encrypted digital data is decrypted by the content key

As is clear from the description above, the digital data of Oishi is encrypted in the storage device by the content key. However, the **content key of Oishi** does **not** teach “a **second block key Kb2 generated on the basis of said second seed,**” as recited by Claim 9, but, instead, the **content key of Oishi**, is **asserted** at page 18 of the outstanding Office Action itself, **as teaching the second seed**. Thus, Oishi fails to teach “**generating**, outside the information-recording medium, an **encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed**,” as recited by Claim 9.

Further, if the content key is asserted as a second block key Kb2, instead of as the second seed, Applicants submit that the content key is not described by Oishi as “generated

on the basis of said second seed,” defined as generated “outside the information-recording medium...on the basis of a first block key Kb1 generated on the basis of said first seed.”

Because, as discussed above, Oishi does not cure the deficiencies of Asano1 that are conceded by the outstanding Office Action with regard to Claim 9, Applicants respectfully request that the rejection under 35 U.S.C. § 103(a) of Claim 9 and Claims 10-13, which depend therefrom, be withdrawn.

Conclusion

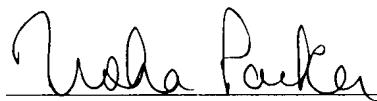
In light of the above discussion, the present application is believed to be in condition for allowance. An early and favorable action to that effect is respectfully requested.

Further, Applicants repeat the request that the arguments submitted herein and the previously filed remarks regarding proper combinations be fully considered, especially if a rearrangement of already-cited references or an addition of a reference to the present combinations of references is considered for a subsequent Office Action.

Finally, Applicants encourage the Examiner to contact Applicants’ representatives for any necessary clarification of the claims or arguments herein to advance the prosecution of this application.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Usha Munukutla-Parker
Registration No. 61,939